

Abstract of JP2000059385



PROBLEM TO BE SOLVED: To provide the method for managing plural systems by which plural systems are managed by a single manager even when IP addresses are overlapped.

SOLUTION: In this method for managing plural systems 15, 16 and 17 through one monitor manager 19, each system is provided with a proxy receiving server 30 for mediating the communication between a server machine 18 belonging to that system and the monitor manager and a system ID capable of specifying the system, to which the server machine to become the transmission destination belongs, is added to communication data in the case of communication from the monitor manager to the server machine. The proxy receiving server deletes the system ID from the communication data in the case of communication from the monitor manager to the server machine but adds the system ID capable of specifying the system, to which the server machine as a transmission source belongs, to the communication data in the case of communication from the server machine to the monitor manager.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-59385
(P2000-59385A)

(43) 公開日 平成12年2月25日 (2000.2.25)

| (51) Int.Cl. ⁷ | 識別記号 | F I | デマコト* (参考) |
|---------------------------|-------|---------------|------------|
| H 0 4 L 12/28 | | H 0 4 L 11/00 | 3 1 0 D |
| G 0 6 F 13/00 | 3 5 3 | G 0 6 F 13/00 | 3 5 3 V |
| H 0 4 L 12/56 | | H 0 4 L 11/20 | 1 0 2 D |

審査請求 未請求 請求項の数5 O L (全 11 頁)

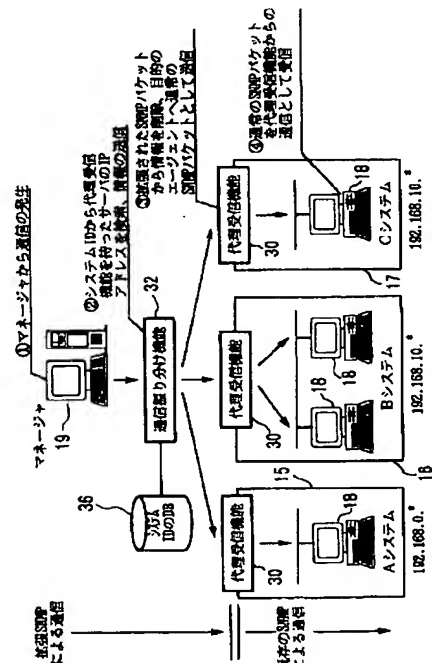
| | | | |
|-----------|----------------------|----------|--|
| (21) 出願番号 | 特願平10-224982 | (71) 出願人 | 000102728 株式会社エヌ・ティ・ティ・データ 東京都江東区豊洲三丁目3番3号 |
| (22) 出願日 | 平成10年8月7日 (1998.8.7) | (72) 発明者 | 櫻井 義晴 東京都江東区豊洲三丁目3番3号 エヌ・ティ・ティ・データ通信株式会社内 |
| | | (74) 代理人 | 100064908 弁理士 志賀 正武 (外9名) |

(54) 【発明の名称】 IPアドレス重複時の複数システム管理方法

(57) 【要約】

【課題】 IPアドレスが重複していても、単一のマネージャによる管理が可能な複数システムの管理方法を提案する。

【解決手段】 複数のシステム15、16、17を一つの監視マネージャ19で管理する方法において、各システムに、システムに属するサーバマシン18と監視マネージャとの通信を仲介する代理受信サーバ30を設け、監視マネージャからサーバマシンへの通信の際に、通信データに、送信先となるサーバマシンが属するシステムを特定できるシステムIDを付加し、代理受信サーバは、監視マネージャからサーバマシンへの通信の際には、通信データからシステムIDを削除し、サーバマシンから監視マネージャへの通信の際には、通信データに、発信元であるサーバマシンが属するシステムを特定できるシステムIDを付加した。



【特許請求の範囲】

【請求項1】 複数の、少なくとも1台以上のサーバマシンを含むシステムを一つの監視マネージャで管理する方法において、

前記システムは、あるシステムに含まれるサーバマシンのIPアドレスと、他のシステムに含まれるサーバマシンのIPアドレスとが重複している場合に、

各システムに、このシステムに属する各サーバマシンと前記監視マネージャとの通信を仲介する代理受信サーバを設け、

前記監視マネージャは、この監視マネージャからサーバマシンへの通信の際に、通信データに、送信先となるサーバマシンが属するシステムを特定できるシステムIDを付加し、

前記代理受信サーバは、監視マネージャからサーバマシンへの通信の際には、通信データから、前記システムIDを削除し、サーバマシンから監視マネージャへの通信の際には、通信データに、発信元であるサーバマシンが属するシステムを特定できるシステムIDを付加することを特徴とするIPアドレス重複時の複数システム管理方法。

【請求項2】 前記通信は、プロトコルとしてSNMPを用い、

前記監視マネージャは、この監視マネージャからサーバマシンへの通信の際に、前記プロトコルに、送信先となるサーバマシンが属するシステムを特定できるシステムIDを付加し、

前記代理受信サーバは、監視マネージャからサーバマシンへの通信の際には、前記プロトコルから前記システムIDを削除し、サーバマシンから監視マネージャへの通信の際には、前記プロトコルに、発信元であるサーバマシンが属するシステムを特定できるシステムIDを付加することを特徴とする請求項1に記載のIPアドレス重複時の複数システム管理方法。

【請求項3】 前記代理受信サーバは、重複することのないIPアドレスをもち、

前記監視マネージャと前記代理受信サーバとの間には、監視マネージャからサーバマシンへの通信の際に、前記システムIDを、このシステムIDに対応するシステムに設けられた代理受信サーバのIPアドレスに変換

する通信振り分けサーバが設けられていることを特徴とする請求項1または2に記載のIPアドレス重複時の複数システム管理方法。

【請求項4】 複数の、少なくとも1台以上のサーバマシンを含むシステムを一つの監視マネージャで管理する方法において、

前記システムは、あるシステムに含まれるサーバマシンのIPアドレスと、他のシステムに含まれるサーバマシンのIPアドレスとが重複している場合に、

サーバマシンから監視マネージャへ障害通知を行う際に、

通知元であるサーバマシンは、障害通知データに、前記サーバマシンが属するシステムを特定できるシステム名を付加することを特徴とするIPアドレス重複時の複数システム管理方法。

【請求項5】 前記通信は、プロトコルとしてSNMPを用い、

サーバマシンから監視マネージャへ障害通知を行う際に、

通知元であるサーバマシンは、前記プロトコルに、前記サーバマシンが属するシステムを特定できるシステム名を付加することを特徴とする請求項4に記載のIPアドレス重複時の複数システム管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、分散システム運用管理方法に関する。

【0002】

【従来の技術】まず、本発明の背景となるTCP/IPとSNMPについて説明する。インターネット上の分散システムにおける通信は、TCP/IP(Transmission Control Protocol/Internet Protocol)と呼ばれるプロトコルを用いて行われる。このTCP/IPでは、IPアドレスを用いてシステム中の個々のマシンが識別されるので、インターネット上では一意なIPアドレスが用いられなければならない。IPアドレスが重複して用いられると、マシンの特定が不可能となり、通信を行うことができない。このIPアドレスの体系を表1に示す。

【表1】

| クラス | 最初の1バイト | ホスト部サイズ | サブネットマスク | 目的 |
|-----|---------|---------|---------------|---------|
| A | 0～27 | 24ビット | 255.0.0.0 | 通常のアドレス |
| B | 128～191 | 16ビット | 255.255.0.0 | 通常のアドレス |
| C | 192～223 | 8ビット | 255.255.255.0 | 通常のアドレス |
| D | 224～239 | *** | *** | マルチキャスト |
| E | 240～255 | *** | *** | 予備 |

表1：IPアドレス体系について

【0003】また、IPアドレスには、インターネットへ

の接続は基本的に不可能であるが、ユーザが自由に利用

することができるアドレスが規定されている。このアドレスは、プライベートIPアドレスと呼ばれる。このプ

イベートIPアドレスの体系を表2に示す。

【表2】

表2：プライベートIPアドレスについて

| クラス | 利用可能アドレス | ネットマスク |
|-----|-----------------------------|-------------|
| A | 10.0.0.0～10.255.255.255 | 255.0.0.0 |
| B | 172.16.0.0～172.32.255.255 | 255.255.0.0 |
| B | 192.168.0.0～192.168.255.255 | 255.255.0.0 |

【0004】次に、SNMP(Simple Network Management Protocol)について説明する。分散システムにおいてマシンの運用管理を行う際には、監視マネージャ(以下マネージャとする)からの集中管理体制を取ることが一般的である。この管理体制を実現するために、分散している各サーバーマシンに、監視エージェント(以下エージェントとする)と呼ばれる監視アプリケーションを常駐させ監視を行う。通常エージェントはイベントドリブン方式を採用しており、エージェントで障害を検出した場合にのみ、マネージャへ情報を通知する。障害を知ったマネージャのオペレータは、詳細な情報を取得するために、マネージャからエージェントへと通信を行う。この手法は、マネージャ・エージェント間のリソースを低減するメリットがあり、広く用いられている。

| | |
|--------------|-----------------------------------|
| TRAP | 障害時等にエージェントが発生させる通信 |
| GET | MIB値の取得 |
| GET NEXT | MIB値の取得(継続) |
| SET | MIB値のセット |
| GET RESPONSE | GET, GET NEXT, SETに対するエージェントからの返事 |

ここで、MIB(Management Information Base)とは、SNMPのエージェントが内部にもつデータベースで、装置の状態を表している。

【0007】エージェントから通信が開始される際のコマンドであるTRAPは、機器に緊急の障害が発生した場合にその情報をマネージャに伝える。マネージャから開始される通信においては、マネージャからのリクエストに対して、該当するMIBの値をマネージャへ返す。なお、マネージャ側からこのMIBの値を変更することにより、装置の該当する機能の状態を変更することもできる。

【0008】図2にSNMPのデータ構造を示す。SNMPは、バージョン1と、Community名2と、PDU3とで構成されている。エージェントから通信が開始される際のコマンドであるTRAPが使用されるときには、前記PDU3に、PDUタイプ4、企業ID5、エージェント・アドレス6、一般TRAP番号7、拡張TRAP番号8、発生時刻9、関連管理情報10が入る。マネージャから通信が開始される際のコマンドであるGET, GET NEXT, SET, GET RESPONSEが使用されるときには、前記PDU3に、PDUタイプ4、リクエスト識別11、エラー・ステータス12、エラー位置番号13、管理情報14等が入る。なお、以下の各図面の説明では、同一の構成には同一の符号を付し、その説明を省

【0005】SNMPは、SNMPネットワーク上の機器の障害等を通知することを目的として設計されたTCP/IP上のプロトコルであり、障害監視等の分野で広く用いられている。SNMPによる通信は、図1(1)に示すエージェントから通信が開始されるTRAPと、図1(2)に示すマネージャから通信が開始されるGET等との2種類に分類することができる。

【0006】SNMPのVersion1では、エージェントから通信が開始される際のコマンドであるTRAPと、マネージャから通信が開始される際のコマンドであるGET, GET NEXT, SETと、マネージャからの通信に対するエージェントからの返信であるGET RESPONSEとの合計5種類のコマンドが定義されている。これら5種類のコマンドの内容を以下に記す。

略する。

【0009】ところで、システム構築時にインターネットへの接続を前提としないシステムでは、インターネットにおいて利用可能なIPアドレスの取得に手間がかかるので、IPアドレスの割り振りについて、自由に利用することの可能なプライベートIPアドレスを利用することが多い。

【0010】図3に、システム構築時には外部と通信する必要の無かった独立したシステムを複数構築した例を示す。図中のAシステム15、Bシステム16、Cシステム17は独立したシステムである。これらのシステムには、1台以上のサーバーマシン18が含まれている。このとき、システム設計のし易さや、構築時の手間等から、含まれているサーバーマシン18のIPアドレス体系が全く同一であるシステムとすることが考えられる。図3では、Bシステム16とCシステム17とが、IPアドレス体系が全く同一となっている。

【0011】また、システムの監視業務を行う場合に、顧客の要望に応じて監視対象システムを追加してゆくことが考えられるが、複数の顧客システムを監視する場合に、一意ではない、重複したIPアドレスが利用されていることも考えられる。

【0012】

【発明が解決しようとする課題】上記のようなシステムに対し、構築後に他のシステムとの接続や統合的な監視が必要となった場合には、図4に示すように、各マシン18で利用されているIPアドレスに重複があるため、監視を行うマネージャ19は、マシン18の一意な識別ができず、TCP/IPを利用した通信が不可能となってしまう。

【0013】TCP/IPによる通信を可能にするには、図5に示すように、通信の代理機能をなすPROXY 20の利用が一般的である。しかし、PROXY 20は一般的な通信路の確保を目的とした技術にすぎず、また、SNMPはその内部にエージェント特定のための情報を保持していないので、以下のような二点の問題がある。第一に、エージェントから障害通知が発生した場合、例えば図5のBシステム16のIPアドレス192.168.10.5のエージェントと、Cシステム17のIPアドレス192.168.10.5を持ったエージェントとの区別がつかず、マネージャ19側で、どのエージェントからの障害通知であるかが判別できない。第二に、マネージャ19側からの通信においても、Bシステム中のエージェントと、Cシステム中のエージェントとを判別できず、PROXY 20が通信を振り分けることができない。

【0014】上記のような問題点に対し、従来技術では二通りの解決方法があった。第一の方法は、図6に示すように、IPアドレスの重複がある顧客システムについては、単一のマネージャによる監視を行わず、それぞれ個別のマネージャ21、22を用意し、お互いにネットワークを干渉させないことで監視を可能とする方法である。しかし、多数の顧客システムを同時に監視する場合には、最悪の場合、監視対象システムと同数のマネージャを用意する必要が生じ、システム面でも人員的にも非効率的な監視を行わねばならないことになる。

【0015】第二の方法は、図7に示すように、重複が起らないようなアドレス体系への変換テーブルを用意し、通信が生じたときに、その通信パケットに対して、発信元・送信先のIPアドレスをこのテーブルによって変換する方法である。この方法によって、単一のマネージャによる監視を可能とすることができる。しかし、この方法では、重複しているIPアドレスを全て新しいIPアドレスへ変換する必要があるため、重複しているIPアドレスと同じ数だけの新たなIPアドレスを用意する必要がある。すると、監視対象システムが増加した場合、IPアドレスが不足し、対応できなくなる可能性がある。

【0016】本発明は、上記の問題を解決するためになされたもので、単一のマネージャによる監視を可能とし、かつ使用されているIPアドレスが重複していても、新しいIPアドレスへ変換する必要がない方法を提案するものである。

【0017】

【課題を解決するための手段】請求項1に記載の発明は、複数の、少なくとも1台以上のサーバマシンを含むシステムを一つの監視マネージャで管理する方法において、前記システムは、あるシステムに含まれるサーバマシンのIPアドレスと、他のシステムに含まれるサーバマシンのIPアドレスとが重複している場合に、各システムに、このシステムに属する各サーバマシンと前記監視マネージャとの通信を仲介する代理受信サーバを設け、前記監視マネージャは、この監視マネージャからサーバマシンへの通信の際に、通信データに、送信先となるサーバマシンが属するシステムを特定できるシステムIDを付加し、前記代理受信サーバは、監視マネージャからサーバマシンへの通信の際には、通信データから、前記システムIDを削除し、サーバマシンから監視マネージャへの通信の際には、通信データに、発信元であるサーバマシンが属するシステムを特定できるシステムIDを付加することを特徴とするIPアドレス重複時の複数システム管理方法である。

【0018】請求項2に記載の発明は、前記通信は、プロトコルとしてSNMPを用い、前記監視マネージャは、この監視マネージャからサーバマシンへの通信の際に、前記プロトコルに、送信先となるサーバマシンが属するシステムを特定できるシステムIDを付加し、前記代理受信サーバは、監視マネージャからサーバマシンへの通信の際には、前記プロトコルから前記システムIDを削除し、サーバマシンから監視マネージャへの通信の際には、前記プロトコルに、発信元であるサーバマシンが属するシステムを特定できるシステムIDを付加することを特徴とする請求項1に記載のIPアドレス重複時の複数システム管理方法である。

【0019】請求項3に記載の発明は、前記代理受信サーバは、重複することのないIPアドレスをもち、前記監視マネージャと前記代理受信サーバとの間には、監視マネージャからサーバマシンへの通信の際に、前記システムIDを、このシステムIDに対応するシステムに設けられた代理受信サーバのIPアドレスに変換する通信振り分けサーバが設けられていることを特徴とする請求項1または2に記載のIPアドレス重複時の複数システム管理方法である。

【0020】請求項4に記載の発明は、複数の、少なくとも1台以上のサーバマシンを含むシステムを一つの監視マネージャで管理する方法において、前記システムは、あるシステムに含まれるサーバマシンのIPアドレスと、他のシステムに含まれるサーバマシンのIPアドレスとが重複している場合に、サーバマシンから監視マネージャへ障害通知を行う際に、通知元であるサーバマシンは、障害通知データに、前記サーバマシンが属するシステムを特定できるシステム名を付加することを特徴とするIPアドレス重複時の複数システム管理方法である。

【0021】請求項5に記載の発明は、前記通信は、プロトコルとしてSNMPを用い、サーバーマシンから監視マネージャへ障害通知を行う際に、通知元であるサーバーマシンは、前記プロトコルに、前記サーバーマシンが属するシステムを特定できるシステム名を付加することを特徴とする請求項4に記載のIPアドレス重複時の複数システム管理方法である。

【0022】

【発明の実施の形態】まず、図9を参照して、本発明の第1実施形態、すなわちサーバーマシン18からマネージャ19への障害の通知を行う場合の構成を説明する。図示したAシステム15、Bシステム16、Cシステム17のように分散したシステムに属するサーバーマシン18を、単一のマネージャ19で集中的に管理するために、各サーバーマシン18に、エージェントと呼ばれる監視アプリケーションを常駐させ監視を行う。エージェントは、このエージェントが常駐するサーバーマシン18の障害を検出した場合に、マネージャ19へ障害情報を通知する。以後、エージェントが常駐するサーバーマシン18を、単に、エージェント18と呼ぶ。

【0023】各システムに属するエージェント18は、システム内においては一意のIPアドレスをもつが、システム外には重複するIPアドレスがある場合がある。本実施形態においては、Bシステムと、Cシステムとは、IPアドレス体系が全く同一となっている。

【0024】Aシステム15、Bシステム16、Cシステム17には、これらのシステムに属するエージェント1

8とマネージャ19との通信を仲介する、代理受信機能30がそれぞれ設けられている。また、マネージャ19は、通信先選択マネージャ31を介して、各システムの代理受信機能30に接続されている。さらに、通信先選択マネージャ31には、仮想-実空間変換テーブルが記憶されているデータベース35が接続されている。

【0025】次に、本実施形態の動作を説明する。マネージャ19とエージェント18との間の通信は、SNMPと呼ばれるプロトコルによって行う。エージェント18は障害を検出した場合に、マネージャ19へ障害情報を通知するが、このとき、SNMPにおいては、TRAPと呼ばれるコマンドを使用する。例えば、Cシステム17のあるエージェント18が障害を検出すると、この情報をTRAP通信として、Cシステム17の代理受信機能30を介して、通信先選択マネージャ31に通知する。

【0026】エージェント18は、TRAP送信時に、図8に示すSNMPのデータ構造中の、関連管理情報10に、システム名23、ホスト名24、大項目25、中項目26、小項目27、状態28、値29といった階層化された障害情報を入れる。図8には、一例として、A商社のホスト(1)においてハードディスクの容量が70パーセントとなった場合の警告を示す。このとき、システム名23=A-SYOUSYA、ホスト名24=HOST(1)、大項目25=HD、中項目26=DISK(1)、小項目27=USAGE、状態28=WARNING、値29=70となる。なお、階層化された障害情報の例を表3に示す。

【表3】

表3：システムの障害を一意に識別するための情報の階層化の例

| システム名 | ホスト名 | 大項目 | 中項目 | 小項目 | 状態 | 値 |
|---------|---------|---------|-----------|------|---------|-----|
| A商社 | HOST(1) | CPU | CPU(1) | 負荷 | Normal | 10 |
| | | | | 負荷平均 | Normal | 30 |
| | | | CPU(2) | 負荷 | Normal | ... |
| | | | | ... | ... | ... |
| | | HD | DISK(1) | 使用容量 | Warning | 50 |
| | | | | 負荷率 | ... | ... |
| | | DISK(2) | ... | ... | ... | |
| | | | ... | ... | ... | |
| | | MEMORY | MEMORY(1) | 使用容量 | Normal | 40 |
| | | | | ... | ... | ... |
| | DB | DB(1) | ... | ... | ... | |
| | | | ... | ... | ... | |
| | DB(2) | ... | ... | 80 | | |
| | | ... | ... | ... | | |
| HOST(2) | CPU | CPU(1) | ... | ... | 50 | |
| | | | ... | ... | ... | |
| B商社 | HOST(3) | CPU | CPU(1) | 負荷 | Normal | 40 |
| | | | | ... | ... | ... |

【0027】通信先選択マネージャ31は、前記の階層化された障害情報を受信すると、この情報に含まれるシステム名23、ホスト名24から発信元のエージェント18を認識し、さらに大項目25、中項目26、小項目27、状態28、値29から障害を特定する。後に続く

動作として、マネージャ19は障害情報のシンボルを変化させるが、通信先選択マネージャ31は、どのシンボルを変化させるかを、データベース35を参照して決定する。

【0028】この決定をもとに、マネージャ19は、図

10に示す該当する障害情報のシンボルを変化させ、障害情報の表示を行う。以上の方法により、マネージャ19のオペレータは、エージェント18のIPアドレスに重複がある場合であっても、発信元のエージェントを特定できる。

【0029】次に、図12、および図14を用いて、本発明の第2実施形態、すなわちマネージャ19からエージェント18へのリクエスト通信、およびこれに対するエージェント18からマネージャ19への返信を行う場合の構成を説明する。

【0030】前記の障害を知ったマネージャ19のオペレータは、詳細な情報を取得するために、マネージャ19からエージェント18へとリクエスト通信を行い、これに対して、エージェント18は詳細な情報をマネージャ19へ返信する。図12はマネージャ19からエージェント18への通信を示し、図14はこれに対するエージェント18からマネージャ19への返信を示しているが、用いている構成は同一である。

【0031】マネージャ19は、通信振り分け機能32を介して、各システムにそれぞれ設けられた代理受信機能30と接続されている。また、前記通信振り分け機能32には、システムIDのデータベース36が接続されている。また、代理受信機能30には、相互に重複のない、一意のIPアドレスが付けられている。

【0032】本実施形態のSNMPにおいては、GET、GET NEXT、SET、GET RESPONSEといったコマンドが使用される。また、SNMPのデータ構造には、図11に示すように、エージェントIPアドレス33と、システムID34とが付加される。エージェントIPアドレス33とは、各エージェント18に付けられたIPアドレスである。システムID34とは、監視対象システム15、16、17に付けられた一意のID番号である。

【0033】前記システムIDのデータベース36には、表4に示すような、システムID34を対応する代理受信機能30のIPアドレスに変換するためのテーブルが記憶されている。

【表4】

表4：通信振り分け機能が管理するシステムID—代理受信機能のIPアドレス変換テーブル

| システムID | 代理受信機能のIPアドレス |
|--------|---------------|
| 1 | 10.15.1.10 |
| 2 | 10.15.1.11 |
| 3 | 10.15.1.24 |
| 4 | 10.15.1.33 |

上記以外の構成は、第1実施形態と同様である。

【0034】次に、図12、および図13のフローチャートを用いて、マネージャ19からエージェント18へのリクエスト通信(GET等)の動作を説明する。なお、以下の文中に示すS1～S8は、図13のステップを示

す。

【0035】マネージャ19からの通信が発生すると(S1)、送信データとして、エージェントIPアドレス33とシステムID34とが付加された拡張SNMPパケットが作成される(S2)。このパケットが通信振り分け機能32に送られると、この通信振り分け機能32は、システムIDのデータベース36に記憶されている変換テーブルを参照し、システムID34を代理受信機能30のIPアドレスに変換する(S3)。そして、このIPアドレスが登録されたものであるかが確認され(S4)、登録されていない場合は、通信障害をマネージャ19に通知する(S5)。登録されていれば、変換されたIPアドレスをもつ代理受信機能30へパケットを送信する(S6)。

【0036】該当するIPアドレスをもつ代理受信機能30が、前記拡張SNMPパケットを受信すると、このパケットからエージェントIPアドレス33とシステムID34とを削除し(S7)、送信先のエージェント18へ、通常のSNMPパケットとして送信する。そして、エージェント18は、通常のSNMPパケットを受信する(S8)。従って、この方法では、エージェント18は通常のSNMPパケットを受信できる機能をもっていればよいので、従来からあるエージェントに対して、特別な変更をする必要はない。

【0037】次に、図14、および図15のフローチャートを用いて、マネージャ19からのリクエストに対する、エージェント18からマネージャ19への返信(GET RESPONSE)の動作を説明する。なお、以下の文中に示すS9～S16は、図15のステップを示す。

【0038】例えば、Cシステム17に属するあるエージェントからの通信が発生すると(S9)、ここから送信された通常のSNMPパケットは、このエージェント18が属するCシステム17の代理受信機能30によって受信される。代理受信機能30は、受信したパケットに、発信元エージェント18のエージェントIPアドレス33およびシステムID34を付加し、拡張SNMPパケットとして(S10)、通信振り分け機能32へ送信する。

【0039】拡張SNMPパケットを受信した通信振り分け機能32は、パケットに付加されたシステムID34が、システムIDのデータベース36に登録された正しいものかどうか確認し、登録されていない不正なものであれば、通信障害をマネージャ19に通知する(S11～S14)。登録された正しいものであれば、パケットをマネージャ19へ送る(S15)。そして、マネージャ19は、拡張SNMPパケットを受信する(S16)。従って、エージェント18からの返信には、プロトコル中にシステムID34が付加されているので、マネージャ19は、どのエージェント18からの返信であるかを一意に特定することができる。

【0040】

【発明の効果】本発明によると、IPアドレスが重複して

いる複数のシステムを単一のマネージャで管理することが可能になった。従って、効率の良い集中的な管理を行うことができるようになった。また、システムの監視業務を行う場合に、顧客の要望等に応じて監視対象システムを追加して、重複したIPアドレスが利用されていたとしても、複数のマネージャを設置する必要はなく、既存資産が活用でき、コストが増加することはない。さらに、このとき、既に多数設置されているエージェントに対して、IPアドレスの変更や、拡張されたSNMPによる通信への対応などの特別な変更をする必要はなく、ユーザは本発明の仕組みを認識する必要もない。

【図面の簡単な説明】

【図1】 SNMPによる通信を示す図。

【図2】 従来のSNMPプロトコルを示す図。

【図3】 IPアドレスの重複したシステムを示す図。

【図4】 IPアドレスの重複により通信が不可能となる例を示す図。

【図5】 従来技術であるPROXY機能により通信を可能とする例を示す図。

【図6】 従来技術である複数マネージャを利用する方法を示す図。

【図7】 従来技術であるアドレス変換による方法を示す図。

【図8】 本発明の第1実施形態によるSNMP TRAPのPDUに対する情報のマッピング例を示す図。

【図9】 本発明の第1実施形態によるエージェントからマネージャへの障害の通知を示す図。

【図10】 本発明の第1実施形態による障害情報のシンボルの状態変化を示す図。

【図11】 本発明の第2実施形態による拡張されたSNMPプロトコルを示す図。

【図12】 本発明の第2実施形態によるマネージャからエージェントへのリクエスト通信を示す図。

【図13】 マネージャからエージェントへのリクエスト通信のフローチャート。

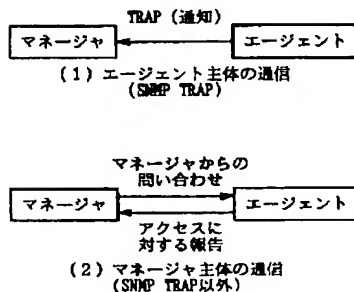
【図14】 本発明の第2実施形態によるマネージャのリクエストに対するエージェントからマネージャへの返信を示す図。

【図15】 マネージャのリクエストに対するエージェントからマネージャへの返信のフローチャート。

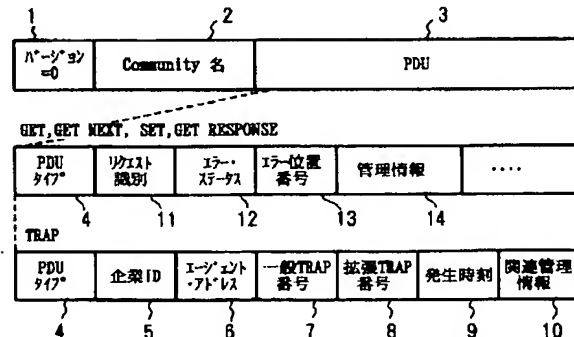
【符号の説明】

| | |
|-----------------|-------------------|
| 1 バージョン | 2 Community名 |
| 3 PDU | 4 PDUタイプ |
| 5 企業ID | 6 エージェント・アドレス |
| 7 一般TRAP番号 | 8 拡張TRAP番号 |
| 9 発生時刻 | 10 関連管理情報 |
| 11 リクエスト識別 | 12 エラー・ステータス |
| 13 エラー位置番号 | 14 管理情報 |
| 15 Aシステム | 16 Bシステム |
| 17 Cシステム | 18 サーバマシン(エージェント) |
| 19 マネージャ | 20 PROXY |
| 21 マネージャ | 22 マネージャ |
| 23 システム名 | 24 ホスト名 |
| 25 大項目 | 26 中項目 |
| 27 小項目 | 28 状態 |
| 29 値 | 30 代理受信機能 |
| 31 通信先選択マネージャ | 32 通信振り分け機能 |
| 33 エージェントIPアドレス | 34 システムID |
| 35 データベース | 36 システムIDのデータベース |

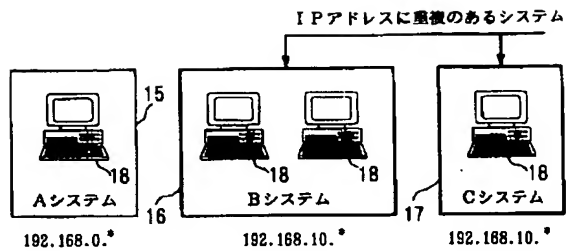
【図1】



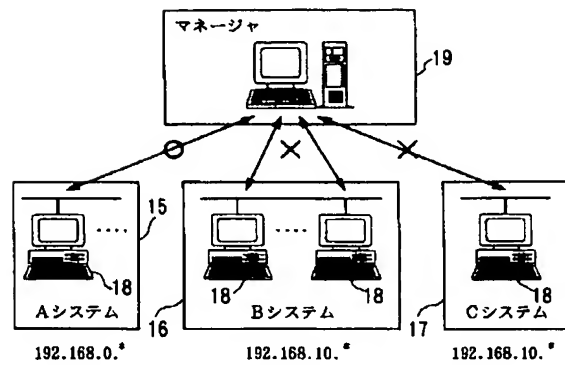
【図2】



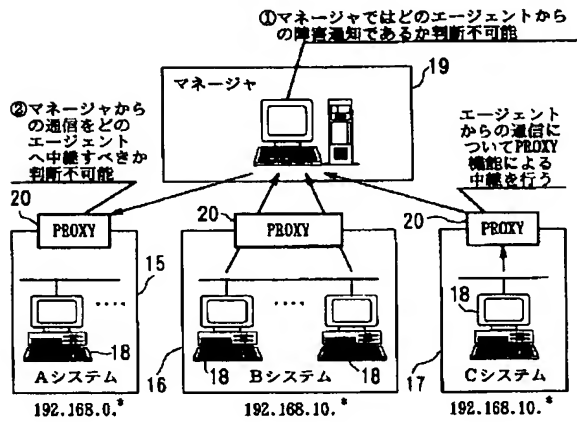
【図3】



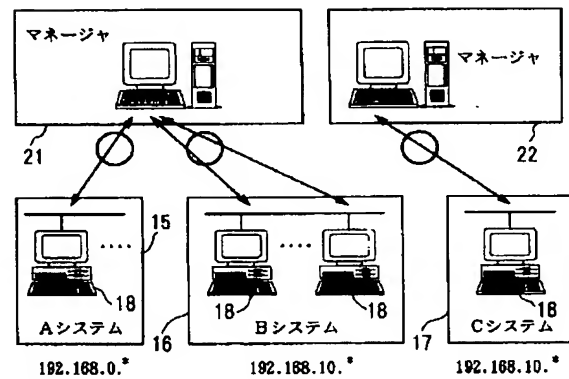
【図4】



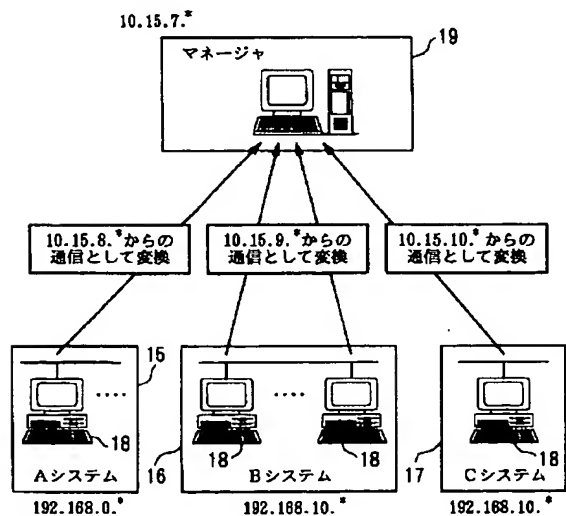
【図5】



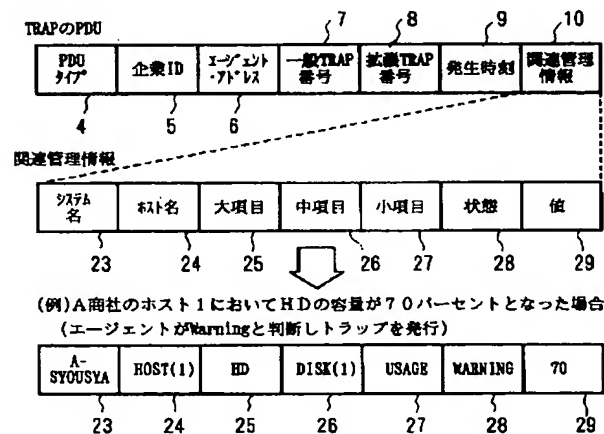
【図6】



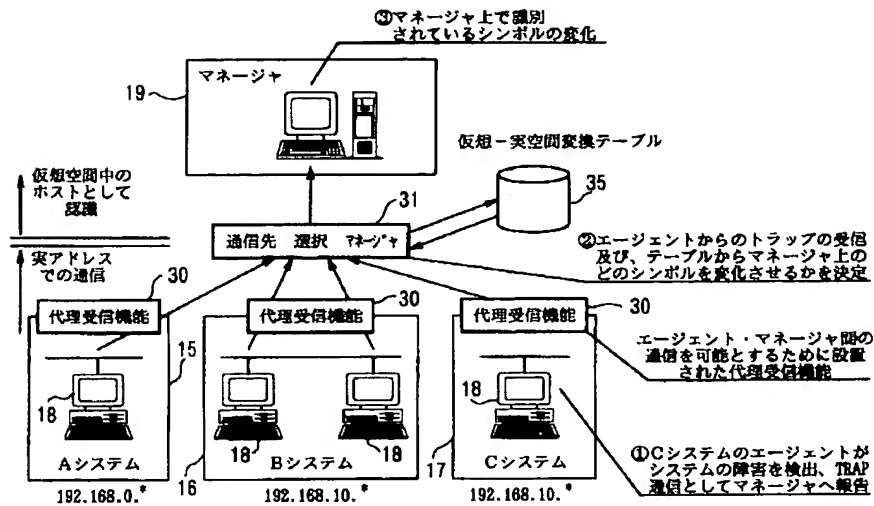
【図7】



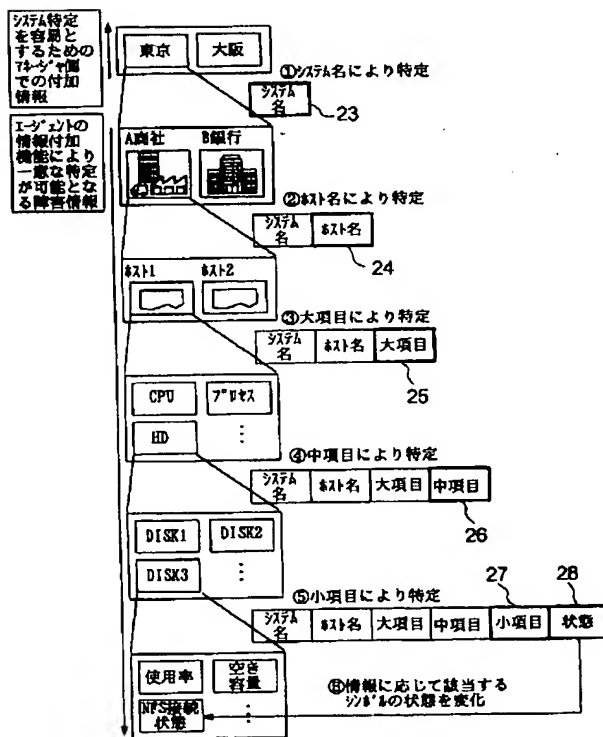
【図8】



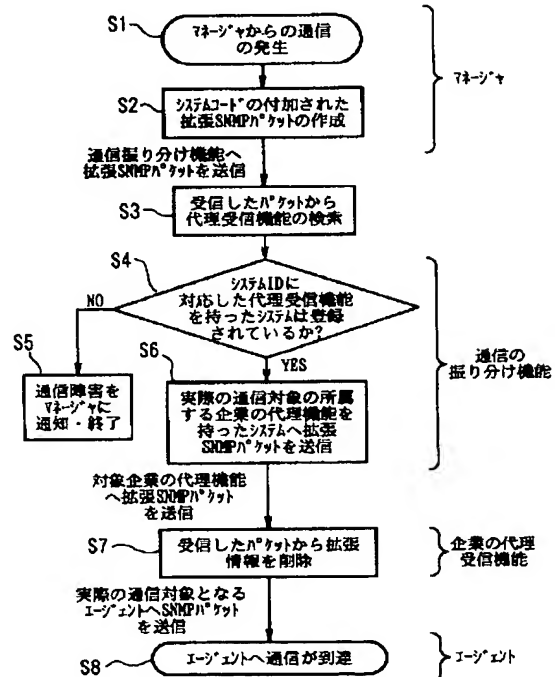
【図9】



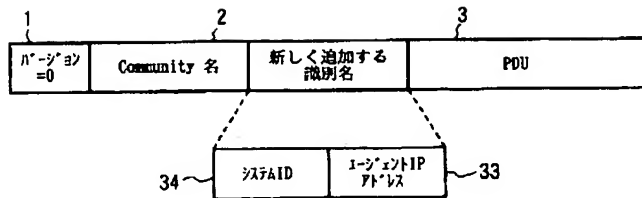
【図10】



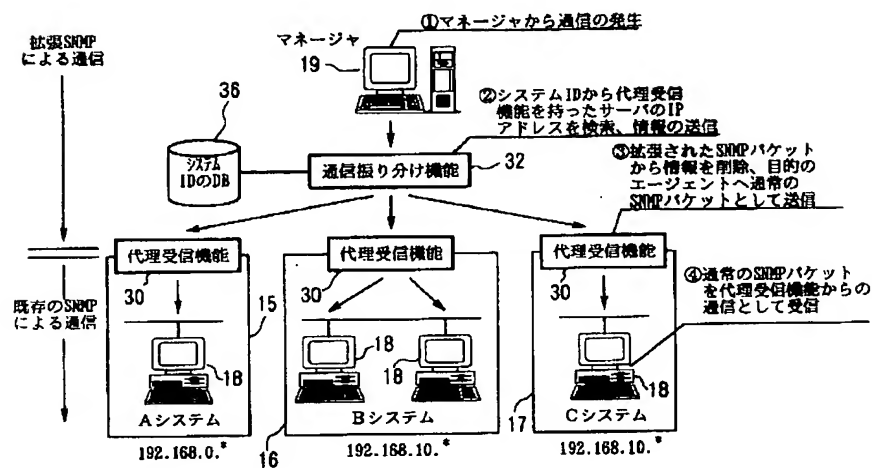
【図13】



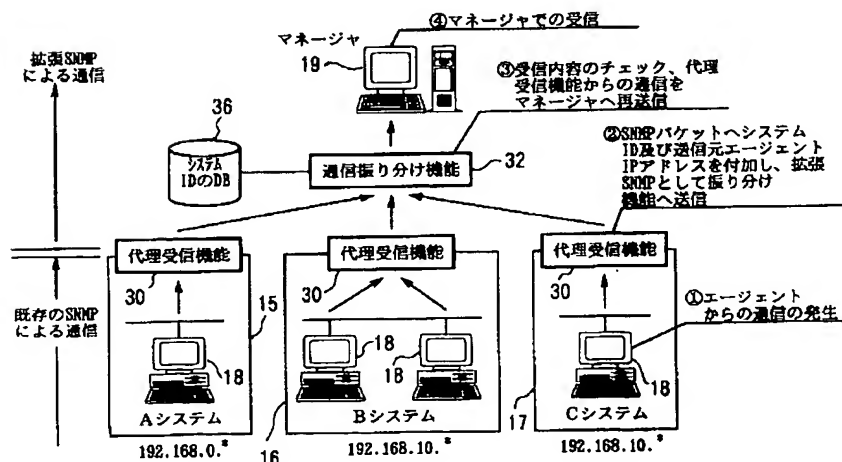
【図11】



【図12】



【図14】



【図15】

